San Isidro, 20 de Noviembre del 2025

RESOLUCION N° 000150-2025-DG/JNJ

VISTOS:

El Informe N° 000278-2025-OTIDG/JNJ de la Oficina de Tecnologías de la Información y Gobierno Digital, el Informe N° 000270-2025-OPM/JNJ de la Oficina de Planeamiento y Modernización, y el Informe N° 000571-2025-OAJ/JNJ de la Oficina de Asesoría Jurídica; y,

CONSIDERANDO:

La Ley de Gobierno Digital, aprobada por el Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece un marco de gobernanza del gobierno digital en las entidades de la Administración Pública, promoviendo la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales para fortalecer la eficiencia y continuidad operativa del Estado;

El Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N.° 029-2021-PCM, en su numeral 109.1 del artículo 109, establece que el Sistema de Gestión de Seguridad de la Información (SGSI), comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

Mediante Resolución Jefatural N° 386-2002-INEI, se aprobó la Directiva Nº 016-2002-INEI/DTNP “Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública”, en cuyo numeral 5.2 del artículo V establece que las Oficinas de Informática (o la que haga sus veces) de las entidades de la administración pública, deben definir un plan de respaldo de la información, de acuerdo a factores legales, institucionales y otros;

Mediante Resolución Nº 097-2025-DG/JNJ se aprobó la Directiva para la formulación, revisión, aprobación, publicación, difusión y derogación de documentos normativos en la Junta Nacional de Justicia;

Mediante Resolución N° 000138-2025-DG/JNJ, de 13 de noviembre de 2025, se aprobó la Guía Técnica para la Gestión de copias de Respaldo de la Información en la Junta Nacional de Justicia, con el objetivo de garantizar el respaldo, almacenamiento y recuperación de la información digital generada por las aplicaciones, sistemas de información y base de datos de la Junta Nacional de Justicia;

Mediante el informe de vistos, la Oficina de Tecnologías de la Información y Gobierno Digital - OTIGD propone el Plan de Respaldo de la Información en la Junta Nacional de Justicia, cuyo objetivo es garantizar el respaldo, almacenamiento y recuperación de la información digital generada por las aplicaciones, sistemas de información y bases de datos de la JNJ, alineado con la Política de Seguridad y los objetivos institucionales; precisando que cumple con las exigencias técnicas, legales y formales establecidas en la normativa vigente y en los instrumentos internos de gestión de la entidad;

Mediante los informes de vistos, la Oficina de Planeamiento y Modernización, y la Oficina de Asesoría Jurídica emiten opinión favorable a la aprobación del Plan de Respaldo de la Información en la Junta Nacional de Justicia, por encontrarse conforme al marco normativo aplicable;

De conformidad con el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; su Reglamento, aprobado por Decreto Supremo N° 029-2021-PCM; la Directiva Nº 016-2002-INEI/DTNP “Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública”, aprobada por la Resolución Jefatural N° 386-2002-INEI; la Directiva para la formulación, revisión, aprobación, publicación, difusión y derogación de documentos normativos en la Junta Nacional de Justicia, aprobada por Resolución Nº 097-2025- DG/JNJ; el Reglamento de Organización y Funciones de la Junta Nacional de Justicia, aprobado por Resolución Nº 036-2024-P-JNJ; y, con el visado de los jefes de las oficinas de Tecnología de la Información y Gobierno Digital, de Planeamiento y Modernización y de Asesoría Jurídica;

SE RESUELVE:

Artículo 1. Aprobar el Plan de Respaldo de la Información en la Junta Nacional de Justicia, que en anexo forma parte integrante de la presente resolución.

Artículo 2. Disponer que la Oficina de Tecnologías de la Información y Gobierno Digital ejecute y supervise las acciones necesarias para la implementación, mantenimiento y seguimiento de las actividades programadas en el referido plan.

Artículo 3. Disponer la publicación de la presente resolución en el Portal de Transparencia y en el Portal Institucional de la Junta Nacional de Justicia (www.gob.pe/jnj).

Regístrese, comuníquese y publíquese.

(documento firmado digitalmente)
KATIA MARIA DEL CARMEN NUÑEZ MARISCAL
DIRECTORA GENERAL
JUNTA NACIONAL DE JUSTICIA

Código	**Versión:**	**Página:**
PL-OTIGD-AST-01	01	Página 1 de 7

Junta Nacional de Justicia

PLAN DE RESPALDO DE LA INFORMACIÓN EN LA JUNTA NACIONAL DE JUSTICIA

Concepto	Nombre y Apellido - Puesto	Firma	Fecha
Elaborado por:	Mario Vallejos Herencia Oficial de Seguridad y Confianza Digital	Firma Digital Firmado digitalmente por VALLEJOS HERENCIA Mario Alberto FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 19.11.2025 15:14:56 -05:00	En firma digital
Elaborado por:	José Alarcón Butrón Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital	Firma Digital Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 19.11.2025 15:31:46 -05:00	En firma digital
Revisado por:	Rafael Sifuentes del Mar Jefe de la Oficina de Planeamiento y Modernización	Firma Digital Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 19.11.2025 15:46:04 -05:00	En firma digital
Aprobado por:	Katia Núñez Mariscal Directora General	Firma Digital Firmado digitalmente por NUÑEZ MARISCAL Katia Maria Del Carmen FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 20.11.2025 14:48:00 -05:00	En firma digital

1. OBJETIVO:

Garantizar el respaldo, almacenamiento y recuperación de la información digital generada por las aplicaciones, sistemas de información y bases de datos de la JNJ, alineado con la Política de Seguridad y los objetivos institucionales.

2. FINALIDAD:

Dotar a la Junta Nacional de Justicia de mecanismos efectivos de resguardo de información que aseguren la continuidad de sus servicios digitales y administrativos frente a incidentes de seguridad, fallas técnicas o desastres, minimizando su impacto.

3. ÁMBITO DE APLICACIÓN:

Incluido: Servidores que albergan sistemas de información, aplicativos y bases de datos; información de unidades de organización almacenada en el servidor de almacenamiento JNJNAS.

Excluido: La información contenida en los discos duros de los equipos de cómputo locales (PCs, laptops, otros) asignados a los colaboradores.

4. CONTROL DE CAMBIOS:

N°	FECHA	NUMERAL	TEXTO MODIFICADO	RESPONSABLE

5. BASE LEGAL:

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado
- Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado mediante Decreto Supremo Nº 016-2024-JUS.
- Decreto Legislativo N°1412, Ley de Gobierno Digital
- Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional De Transformación Digital.
- Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
- Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
- Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva Nº 016-2002-INEI/DTNP “Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública”
- Resolución Directoral Nº 014-2018-INACAL-DN es la que aprobó la Norma Técnica Peruana “NTP-ISO/IEC 31000:2018; Gestión del riesgo. Directrices
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba el uso Obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición”; y

la Norma Técnica Peruana "NTP-ISO/IEC 27005:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición

- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Seguridad de la Información en las Entidades Públicas y en el artículo 3 indica el desarrollo del plan de implementación del SGSI.

6. RESPONSABILIDADES:

Jefes de Unidades de Organización:

- Identificar la información con nivel de criticidad alta, media o baja en sus procesos.
- Solicitar acceso y permisos.

Oficina de Tecnologías de la Información y Gobierno Digital (OTIGD):

- Asegurar y supervisar el cumplimiento de la guía.
- Definir y documentar la periodicidad de respaldos y pruebas.
- Realizar las actividades de recuperación.
- Administrar la herramienta de respaldo (Ej. Veeam Backup).

Servidores Civiles (Usuarios):

- Almacenar la información relevante para sus funciones en las unidades de red y/o carpetas compartidas asignadas.
- Son responsables del contenido en las carpetas que pueden editar.

7. CONTENIDO

7.1 DEFINICIONES:

Para todos los efectos de este documento, se adoptan las definiciones establecidas en la "Guía Técnica para la Gestión de Copias de Respaldo de la Información" (GT-OTIGD-AST-03).

Las definiciones operativas clave para este plan, RPO (Objetivo de Punto de Recuperación) y RTO (Objetivo de Tiempo de Recuperación), se detallan en la sección 7.

7.2 SEGURIDAD Y CIFRADO DE RESPALDOS:

Para asegurar la confidencialidad e integridad de la información de la JNJ, todas las copias de respaldo deben ser gestionadas con estrictas medidas de seguridad, por lo que se establece la obligatoriedad de cifrar la información en sus dos estados críticos:

En reposo: mientras se almacena en los servidores de backup locales o en la nube)

En tránsito: durante su replicación a la sede Miraflores o al proveedor de nube.

Adicionalmente, el acceso a la consola de administración de respaldos (Veeam Backup) y a los propios archivos de respaldo estará restringido únicamente al personal de OTIGD autorizado, garantizando que solo los especialistas designados puedan ejecutar operaciones de consulta o restauración.

7.3 ESTRATEGIA Y DEFINICIÓN DE OBJETIVOS RPO y RTO

El plan se basa en los niveles de criticidad definidos en la GT-OTIGD-AST-03 (Guía Técnica para la Gestión de Copias de Respaldo)

RPO (Objetivo de Punto de Recuperación

Frecuencia y RPO (Objetivo de Punto de Recuperación):

- Bases de Datos (Criticidad Alta): RPO de 24 horas (Backup incremental diario).
- Servidores (Criticidad Alta/Media): RPO de 24 horas (Backup diario a las 00:00).
- Carpetas Compartidas (Criticidad Media): RPO de 24 horas (Backup incremental diario a las 2:00 am).

Período de Retención:

- Servidores Diario: 14 días.
- Servidores Semanal: 4 semanas.
- Servidores Mensual: 3 meses.
- Carpetas Compartidas (Diario): 15 días.
- Bases de Datos (Diario Incremental): 7 días.
- Bases de Datos (Semanal Full): 4 semanas.

Almacenamiento y Estrategia 3-2-1:

- 3 Copias: Producción + Copia Local + Copia fuera de sitio.
- 2 Soportes:
- Copia Primaria: Servidor de copias de respaldo local y Servidor Veeam Backup.
- Copia Secundaria: Nube contratada y/o sede Miraflores.
- 1 Copia fuera de sitio: Se mantienen respaldos de información crítica con una copia fuera de sitio (sede Miraflores y/o nube contratada):

Nivel 1 (Recuperación Rápida fuera de sitio): Las copias de respaldo semanales (Full) se replican a la sede Miraflores para una recuperación rápida en caso de desastre en la sede principal.

Nivel 2 (Archivo a Largo Plazo): Las copias de respaldo mensuales (Full) se almacenan en la sede Miraflores y/o nube pública contratada para archivado histórico y recuperación en caso de un desastre regional que afecte ambas sedes.

Frecuencia: Mínimo semanal para la réplica a Miraflores.

RTO (Objetivo de Tiempo de Recuperación)

El tiempo máximo aceptable para restaurar un servicio o datos después de un incidente dependiendo de su nivel de criticidad:

- **Alta:** Información vital para la continuidad operativa de procesos críticos. RTO de **4 horas**
- **Media:** Información que puede ser recuperada en un periodo de tiempo razonable. RTO de **24 horas**
- **Baja:** Información que no afecta las operaciones normales. RTO de **72 horas**

7.4 PRUEBAS DE RESPALDO Y RECUPERACIÓN:

Verificación de Tareas: Diaria, como parte de la supervisión de la OTIGD.

- Responsable: El Administrador de Sistemas de la OTIGD.
- Frecuencia: Diaria (al inicio de la jornada laboral).
- Procedimiento: Se realizará la revisión de los registros (logs) y alertas de la herramienta de respaldo (Veeam Backup) para confirmar la correcta ejecución de todas las tareas programadas. Cualquier fallo debe ser escalado y resuelto en un plazo no mayor a 8 horas.

Pruebas de Restauración:

- Frecuencia: Mensual (como indica la Guía) y/o a solicitud.
- Procedimiento: Se seleccionará aleatoriamente un (1) servidor, una (1) base de datos y un (1) conjunto de archivos de carpetas compartidas para una restauración completa en un entorno de pruebas.
- Registro: Todas las pruebas de restauración (exitosa o fallida) deben documentarse en un Registro de Pruebas de Restauración, detallando el activo, la fecha, el tiempo de restauración (para medir el RTO) y las lecciones aprendidas.

7.5 PROCEDIMIENTO DE SOLICITUD DE RECUPERACIÓN DE INFORMACIÓN

- Toda solicitud de recuperación de datos debe ser canalizada por el/la jefe de la unidad de organización o, en su defecto, un servidor civil designado.
- La solicitud se debe presentar formalmente a través del Sistema de Gestión Documental.
- La solicitud debe incluir:
- Nombre y ruta exacta del archivo/carpeta/sistema.
- Fecha y hora aproximada de la versión que se desea recuperar.
- Motivo de la solicitud.
- La OTIGD atenderá la solicitud en base a los RTO definidos

7.6 COMUNICACIÓN Y CONCIENTIZACIÓN

Para asegurar el cumplimiento del alcance de este Plan, la OTIGD empleará las siguientes acciones de concientización, tal como lo requiere la Guía Técnica:

- Campañas semestrales: Se enviarán comunicados recordatorios a todos los servidores civiles sobre la política de almacenar toda información relevante en las unidades de red asignadas.
- Inducción: Se incluirá esta política en el proceso de inducción de nuevos servidores civiles.
- Avisos: Se configurará un aviso periódico recordando esta obligación.

8. ACTIVIDADES PROGRAMADAS

Para el cumplimiento de los objetivos del Plan, se establecen las siguientes metas operativas:

Actividad	Unidad de Medida	Meta Programada	Responsable
Ejecución de Copias de Respaldo (Diarias)	Reporte de Backup	100% de éxito diario	Infraestructura OTIGD
Pruebas de Restauración (Aleatorias)	Informe de Prueba de Restauración	4 pruebas al año (Trimestral)	Infraestructura OTIGD
Réplica de Información a Sitio Alterno	Reporte de Replicación	100% de éxito semanal	Infraestructura OTIGD

Campañas de Concientización	Comunicado	2 campañas al año (Semestral)	Infraestructura OTIGD

9. SEGUIMIENTO Y EVALUACIÓN

La Oficina de Tecnologías de la Información y Gobierno Digital es la encargada de realizar el seguimiento a la ejecución del presente Plan.

Reporte de Cumplimiento: El responsable de Infraestructura elevará semestralmente un reporte de estado a la Jefatura de la OTIGD, detallando:

- El porcentaje de cumplimiento de las tareas de respaldo (éxito de backups).
- Los resultados de las pruebas de restauración mensuales ejecutadas.
- El análisis de incidentes de pérdida de datos y tiempos de recuperación alcanzados.
- El estado de la capacidad de almacenamiento y proyección de requerimientos técnicos.